DETAILED ACTION

1. This Office Action is in response to the application 10/500,792 filed on 03/21/2005.

2. Claims 1-11 have been examined and are pending.

Specification

3. The disclosure is objected to because of the following informalities:

- The "item 20," in Fig. 1, is used for three different elements as described in the specification: "calculation means 20" *(pars. 0079-0080),* "server 20" *(pars. 0082-0083, 0086, and 0089),* and "the memory space 20" *(par. 0091).* Appropriate corrections are required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. **Claims 6 and 10 are rejected under 35 U.S.C. 101** because the claims may be directed to non-statutory subject mater.

- **Regarding claim 6**, although the preamble of the claim recites "*cryptographic apparatus,*" the body of the claim may be directed to software implementation since the "*calculation means,*" "*asymmetric keys,*" and "*symmetric keys,*" could be implemented by software by one of ordinary skill in the art at the time the invention was made. Therefore, the claimed subject matter does not belong to any of the four statutory categories set forth above.

- **Regarding claim 10**, although the preamble of the claim recites "*cryptographic system,*" the body of the claim may be directed to software implementation since the they do not recite any elements of hardware; "*calculation means,*" "*asymmetric keys,*" and "*symmetric keys,*" could be implemented by software by one of ordinary skill in the art at the time the invention was made. Therefore, the claimed subject matter does not belong to any of the four statutory categories set forth above.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. **Claims 1-11 are rejected under 35 U.S.C. 112, second paragraph**, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- **Regarding claims 1, 6, 10, and 11**, the claims recite "***n*** *members;"* however, '**n**' is not explicitly defined.

- **Regarding claims 2-5 and 7-9**, these claims are dependent on claims 1 and 6, respectively, and therefore inherit the 35 U.S.C 112 issues of the independent claims.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention

> was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

10. **Claims 1 and 10-11 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Camenisch, "*Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem,*" Doctor of Technical Science, Swiss Federal Institute of Technology Zurich, 1998, and in view of Inada, U.S. Patent No. 6,986,044, filed on August 31, 1999, and further in view of Kim et al. (hereinafter "Kim"), "Efficient and Secure Member Deletion in Group Signature Schemes," D. Won (Ed): ICISC 2000, LNCS 2015, pp. 150-160, Springer-Verlag Berlin Heidelberg, 2001.

- **Regarding claim 1**, Camenisch discloses a cryptographic method of anonymously signing a message by a member of a group comprising n members each equipped with calculation means (25) and associated storage means (24), which method is characterized in that it comprises the following initial steps at the time of constituting the group *(page 71, lines 4-18)*:

a first step in which first calculation means of a trusted authority calculate a pair of asymmetric keys (30, 31) common to the members of the group and comprising a common public key (30) and a common private key (31) (operation 1) *(page 100, section 5.4.1, lines 19-21; page 105, section 5.5.1, lines 16-17; RSA public key (n,e), the primes p and q are her secret key)*,

a second step in which the first calculation means calculate a group public key (32) associated with the group (operation 2) *(page 101, lines 1-3; page 105, section 5.5.1, lines 29-30; group public key Y)*,

a third step in which, for each member, during an interaction between the calculation means of the trusted authority and the calculation means of the member, a group private key (33_1) is calculated (operation 3) and stored (operation 4) in the storage means (24) of the member, each group private key (33_1) being associated with the group public key (32) and being different for each member of the group *(pages 101-102, section 54.2; pages 106-107, section 5.5.2: Generating Membership Keys and Certificate; Arto joins the group, obtains membership certificate, stores x, y, and v securely),*

a fourth step in which the first calculation means determine as many symmetrical secret keys (34_i) as there are members of the group (operation 5) *(page 74, lines 13-15; a secret key x_i to each group member P_i)*, and

the following steps on the group member anonymously signing (operation 10) a message having to be sent to an addressee:

a ninth step in which the member's calculation means (25) calculate (operation 12) an anonymous signature of the message using its group private key (33_1) *(pages 102-103*

and 107-108; sections 5.4.3, 5.4.4, 5.5.3, and 5.5.4; signing messages and opening signature), and

a tenth step in which the member's calculation means (24) calculate (operation 13) an additional signature of the combination comprising the message and the anonymous signature using the member's common private key (31) *(pages 102-103 and 107-108; sections 5.4.3, 5.4.4, 5.5.3, and 5.5.4; signing messages and opening signature)*.

Camenisch does not explicitly disclose a fifth step in which the first calculation means (20) encrypt the common private key (31) using each of the secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members (operation 6), a seventh step in which the first calculation means (20) encrypt the common private key (31) using each of the secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members (operation 9), and an eighth step in which the common private key (31) stored by the storage means (24) of the member is updated (operation 11) only if one of the encrypted values of the common private key (31) may be decrypted using the symmetrical secret key (34_1) in the member's storage means (24).

However, in an analogous art, Inada discloses a method for group unit encryption/decryption, wherein:

a fifth step in which the first calculation means (20) encrypt the common private key (31) using each of the secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members (operation 6) *(col. 19, lines 10-13; common key C_G is encrypted using P_{Mi} key)*,

a seventh step in which the first calculation means (20) encrypt the common private key (31) using each of the secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members (operation 9) *(col. 19, lines 10-13; common key C_G is encrypted using P_{Mi} key)*, and

an eighth step in which the common private key (31) stored by the storage means (24) of the member is updated (operation 11) only if one of the encrypted values of the common private key (31) may be decrypted using the symmetrical secret key (34_1) in the member's storage means (24) *(col. 22, lines55-60; the extracted $P_{Mi}(C_G)$ is decrypted by use of the individual key to acquire the common key C_G)*,

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Inada with that of Camenisch wherein a fifth step in which the first calculation means (20) encrypt the common private key (31) using each of the secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members (operation 6), a seventh step in which the first calculation means (20) encrypt the common private key (31) using each of the secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members (operation 9), and an eighth step in which the common private key (31) stored by the storage means (24) of the member is updated (operation 11) only if one of the encrypted values of the common private key (31) may be decrypted using the symmetrical secret key (34_1) in the member's storage means (24) to allow an arbitrary member in a group to decrypt and write a signature by use of a group key which is allowed to be used by only the group member *(col. 1, lines 9-12)*.

Camenisch and Inada do not explicitly disclose it comprises the following steps on each revocation within the group: a sixth step in which the first calculation means (20) modify the pair of common asymmetric keys (31) to determine a common public key (30) and a common private key (31) that are up to date (operation 8).

However, in an analogous art, Kim discloses a method for efficient and secure member deletion in group signature schemes, wherein in that it comprises the following steps on each revocation within the group: a sixth step in which the first calculation means (20) modify the pair of common asymmetric keys (31) to determine a common public key (30) and a common private key (31) that are up to date (operation 8) *(page 157; section 1.3; steps 1-3)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Kim with that of Camenisch and Inada wherein in that it comprises the following steps on each revocation within the group: a sixth step in which the first calculation means (20) modify the pair of common asymmetric keys (31) to determine a common public key (30) and a common private key (31) that are up to date (operation 8) to allow member deletion and sign-tracing generated by a specific member *(page 151, lines 15-16)*.

- **Regarding claim 10**, Camenisch discloses a cryptographic system for anonymously signing a digital message by implementing a method according to claim 1, characterized in that it comprises at least: first calculation means (20) for calculating (operations 1, 2) at least one of said pair of asymmetric keys (30, 31) common to the members of the group of n members *(page 100, section 5.4.1, lines 19-21; page 105, section*

5.5.1, lines 16-17; RSA public key (n,e), the primes p and q are her secret key) and said group public key (32) associated with the group *(page 101, lines 1-3; page 105, section 5.5.1, lines 29-30; group public key Y)*, for calculating (operation 3) said group private key (33_1) for each member during interaction with the member's calculation means (25), each said group private key (33_1) being associated with said group public key (32) and being different for each member of the group *(pages 101-102, section 54.2; pages 106-107, section 5.5.2: Generating Membership Keys and Certificate; Arto joins the group, obtains membership certificate, stores x, y, and v securely)*, for determining (operation 5) as many of said symmetrical secret keys (34_i) as there are members of the group *(page 74, lines 13-15; a secret key x_i to each group member P_i)*, and storing said private key (31) common to the members of the group, said group private key (33_1) of the member, and said symmetrical secret key (34_1) assigned to the member *(pages 101-102, section 54.2; pages 106-107, section 5.5.2: Generating Membership Keys and Certificate; Arto joins the group, obtains membership certificate, stores x, y, and v securely)*, and calculation means (25) for calculating (operation 12) an anonymous signature for a message using its said group private key (33_1) and for calculating (operation 13) an additional signature for the combination comprising the message and the anonymous signature using the member's said common private key (31) *(pages 102-103 and 107-108; sections 5.4.3, 5.4.4, 5.5.3, and 5.5.4; signing messages and opening signature)*.

Camenisch does not explicitly disclose encrypting (operation 6) said common private key (31) using each of said symmetrical secret keys (34_i) to obtain as many

encrypted forms of said common private key (31) as there are non-revoked members; and as many smart cards (21_1) as there are members in the group.

However, in an analogous art, Inada discloses a method for group unit encryption/decryption, wherein encrypting (operation 6) said common private key (31) using each of said symmetrical secret keys (34_i) to obtain as many encrypted forms of said common private key (31) as there are non-revoked members *(col. 19, lines 10-13; common key C_G is encrypted using P_{Mi} key; col. 22, lines55-60; the extracted $P_{Mi}(C_G)$ is decrypted by use of the individual key to acquire the common key C_G)*; and as many smart cards (21_1) as there are members in the group *(col. 1, lines 52-55 and 65-67)*.

Camenisch and Inada do not explicitly disclose means (25) for updating said common private key (31) stored in the member's storage means (34) to update (operation 11) said common private key (31) only if one of the encrypted values of said common private key (31) calculated by said first calculation means (20) of the apparatus may be decrypted using said symmetrical secret key (34_1) in said member's storage means (24).

However, in an analogous art, Kim discloses a method for efficient and secure member deletion in group signature schemes, wherein means (25) for updating said common private key (31) stored in the member's storage means (34) to update (operation 11) said common private key (31) only if one of the encrypted values of said common private key (31) calculated by said first calculation means (20) of the apparatus may be decrypted using said symmetrical secret key (34_1) in said member's storage means (24) *(page 157; section 1.3; steps 1-3)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Kim with that of Camenisch and Inada wherein means (25) for updating said common private key (31) stored in the member's storage means (34) to update (operation 11) said common private key (31) only if one of the encrypted values of said common private key (31) calculated by said first calculation means (20) of the apparatus may be decrypted using said symmetrical secret key (34_1) in said member's storage means (24) to allow member deletion and sign-tracing generated by a specific member *(page 151, lines 15-16)*.

- **Regarding claim 11**, claim 11 is similar in scope to claim 1, and is therefore rejected under similar rationale.

11. **Claims 6-9 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Camenisch, "*Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem,*" Doctor of Technical Science, Swiss Federal Institute of Technology Zurich, 1998, and in view of Inada, U.S. Patent No. 6,986,044, filed on August 31, 1999.

- **Regarding claim 6**, Camenisch discloses cryptographic apparatus for anonymously signing a digital message *(page 71, lines 4-18)*, characterized in that it comprises:

first calculation means (20) for calculating (operations 1, 2) at least one pair of asymmetric keys (30, 31) common to the members of the group of n members) *(page 100, section 5.4.1, lines 19-21; page 105, section 5.5.1, lines 16-17; RSA public key (n,e), the primes p and q are her secret key)* and a group public key (32) associated with the group, for

calculating (operation 3) a group private key (33_1) *(page 101, lines 1-3; page 105, section 5.5.1)* for each member during interaction with the member's calculation means (25), each group private key (33_1) being associated with the group public key (32) *(pages 101-102, section 54.2; pages 106-107, section 5.5.2: Generating Membership Keys and Certificate; Arto joins the group, obtains membership certificate, stores x, y, and v securely)* and being different for each member of the group, for determining (operation 5) as many symmetrical secret keys (34i) *(page 74, lines 13-15; a secret key x_i to each group member P_i)* as there are members of the group.

Camenisch does not explicitly disclose encrypting (operation 6) the common private key (31) using each of the symmetrical secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members.

However, in an analogous art, Inada discloses a method for group unit encryption/decryption, wherein encrypting (operation 6) the common private key (31) using each of the symmetrical secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members *(col. 19, lines 10-13; common key C_G is encrypted using P_{Mi} key)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Inada with that of Camenisch wherein disclose encrypting (operation 6) the common private key (31) using each of the symmetrical secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members to allow an arbitrary member in a group

to decrypt and write a signature by use of a group key which is allowed to be used by only the group member *(col. 1, lines 9-12)*.

- **Regarding claim 7**, Camenisch and Inada disclose cryptographic apparatus according to claim 6 for anonymously signing a digital message.

Camenisch further discloses storage means (36) connected to the first calculation means (20) via a communications network (23) for storing at least an symmetrical secret key (34_i) of each member of the group, the group public key (32), the public key (30) common to the members of the group, and each of the different encrypted forms of the common private key (31) *(pages 101-102, section 54.2; pages 106-107, section 5.5.2: Generating Membership Keys and Certificate; Arto joins the group, obtains membership certificate, stores x, y, and v securely)*.

- **Regarding claim 8**, Camenisch and Inada discloses a smart card (21_1) *(Inada: col. 1, lines 52-55 and 65-67)* intended for a member of a group of n members and adapted to interact with apparatus according to either claim 6 or claim 7, characterized in that it comprises:

Camenisch further discloses means (24) for storing a private key (31) common to the members of the group, a group private key (33_1) of the member, and a symmetrical secret key (34_1) assigned to the member *(pages 101-102, section 54.2; pages 106-107, section 5.5.2: Generating Membership Keys and Certificate; Arto joins the group, obtains membership certificate, stores x, y, and v securely)*, and calculation means (25) for calculating (operation 12) an anonymous signature for a message using its group private key (33_1) and for calculating (operation 13) an additional signature for the combination

comprising the message and the anonymous signature using the member's common private key (31) *(pages 102-103 and 107-108; sections 5.4.3, 5.4.4, 5.5.3, and 5.5.4; signing messages and opening signature)*.

Inada further discloses means (25) for updating the common private key (31) stored in the member's storage means (34) to update (operation 11) the common private key (31) only if one of the encrypted values of the common private key (31) calculated by the first calculation means (20) of the apparatus may be decrypted using the symmetrical secret key (34_1) in the member's storage means (24) *(col. 19, lines 10-13; common key C_G is encrypted using P_{Mi} key)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Inada with that of Camenisch to include means (25) for updating the common private key (31) stored in the member's storage means (34) to update (operation 11) the common private key (31) only if one of the encrypted values of the common private key (31) calculated by the first calculation means (20) of the apparatus may be decrypted using the symmetrical secret key (34_1) in the member's storage means to allow an arbitrary member in a group to decrypt and write a signature by use of a group key which is allowed to be used by only the group member *(col. 1, lines 9-12)*.

- **Regarding claim 9**, Camenisch and Inada discloses a smart card (21_1) *(Inada: col. 1, lines 52-55 and 65-67)* according to claim 8.

Inada further discloses the updating means (25) comprises decrypting means for decrypting one of the encrypted values of the common private key (31) calculated (operation

1) by the first calculation means (20) of the apparatus using the symmetrical secret key (34_1) in the member's storage means (24) *(col. 22, lines55-60; the extracted $P_{Mi}(C_G)$ is decrypted by use of the individual key to acquire the common key C_G)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Inada with that of Camenisch to include updating means (25) comprises decrypting means for decrypting one of the encrypted values of the common private key (31) calculated (operation 1) by the first calculation means (20) of the apparatus using the symmetrical secret key (34_1) in the member's storage means (24) to allow an arbitrary member in a group to decrypt and write a signature by use of a group key which is allowed to be used by only the group member *(col. 1, lines 9-12)*.

Allowable Subject Matter

- **Claims 2, 3, and 5 are objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

- **Claim 4 is objected to** as being dependent upon a rejected base claim. Claim 4 is dependent on claim 3, and would be allowable if claim 3 is rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137